ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 6, June 2014

Review of Attacks on MANETS

Gagandeep Kaur[1], Dr.Navdeep Kaur[2]

[1]M-Tech Student, Computer Science, Sri Guru Granth Sahib World University, Fatehgarh Sahib, India

[2]Head of Department, Computer Science, Sri Guru Granth Sahib World University, Fatehgarh Sahib, India

ABSTRACT: Mobile Ad-hoc Network (MANET) is used most commonly all around the world, because it has the ability to communicate each other without any fixed network. Each mobile node can move freely in any direction and changes their links to other devices. Security is an essential part of ad hoc networks. Due to its dynamic topology, no centralized infrastructure, resource constraints and limited security it is vulnerable to various attacks Black hole and Gray hole attack is one of them. When the malicious node advertises itself as having the shortest path to the destination and falsely replies to the route requests and drops all receiving packets .In this paper various attacks on AODV routing protocol are discussed and reviewed. The basic aim is to study various attacks and there effects to network, so that we can predict the type of attack and recover from attack.

Keywords: MANETS, AODV, NS2, ATTACKS, BLACK HOLE

I. INTRODUCTION

A Mobile Ad-hoc Network (MANET) [15] can be defined as collection of mobile nodes. It does not rely on any fixed infrastructure. Since it is an infrastructure e less network, the mobile nodes in the network dynamically setup paths among themselves to transmit packets from the source to destination and it is a self-configuring network. MANET can be used in different applications such as battlefield communication, emergency relief scenario, disaster areas and outdoor activities, etc. The nature of MANET is a dynamically changing process, due to its dynamically changing process its vulnerable for wide range of attack. A MANET is a multi-hop wireless network that is formed dynamically from an accumulation of mobile nodes without the assistance of a centralized coordinator. As the radio propagation range is limited, each mobile node has only limited information, such as its own ID and the Medium Access Control (MAC) address of its one-hop neighbour's. Therefore, if two nodes are not within the radio propagation range, a multi-hop, via one or more intermediate nodes, is required to forward packets. With recent performance advancement in wireless technology, portable computing platforms and small wireless devices become indispensable devices of our daily life. The use of a portable device is constrained by its energy, making power conservation the most critical issue for portable devices and their applications.

a. AODV Routing Protocol

The Ad Hoc On-Demand Distance Vector (AODV) routing protocol [14] is an adaptation of the DSDV protocol for dynamic link conditions. Every node in an Ad-hoc network maintains a routing table, which contains information about the route to a particular destination. Whenever a packet is to be sent by a node, it first checks with its routing table to determine whether a route to the destination is already available. If so, it uses that route to send the packets to the destination. If a route is not available or the previously entered route is inactivated, then the node initiates a route discovery process. A RREQ (Route Request) packet is broadcasted by the node. Every node that receives the RREQ packet first checks if it is the destination for that packet and if so, it sends back an RREP (Route Reply) packet. If it is not the destination, then it checks with its routing table to determine if it has got a route to the destination. If not, it relays the RREQ packet by broadcasting it to its neighbours. If its routing table does contain an entry to the destination, then the next step is the comparison of the 'Destination Sequence' number in its routing table to that present in the RREQ packet. This Destination Sequence number is the sequence number of the last sent packet from the destination to the source. If the destination sequence number present in the routing table is lesser than or equal to the one contained in the RREQ packet, then the node relays the request further to its neighbours. If the number in the routing table is higher than the number in the packet, it denotes that the route is a 'fresh route' and packets can be sent through this route. This intermediate node then sends a RREP packet to the node through which it received the RREQ packet. The RREP

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 6, June 2014

packet gets relayed back to the source through the reverse route. The source node then updates its routing table and sends its packet through this route. During the operation, if any node identifies a link failure it sends a RERR (Route Error) packet to all other nodes that uses this link for their communication to other nodes.

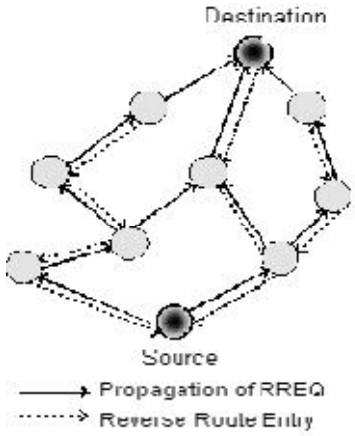


Fig.1 AODV routing

II. RELATED WORK

H. Deng [2] proposed the method for detecting the single black hole node in MANET. In this method, the intermediate nodes send RREP message along with the next hop information. After getting this information, the source node sends further request to next hop node to verify that it has the route to the intermediate node or not. If the route exists, the intermediate node is trusted and source node will send data packets via that trusted node. If not, the reply message from intermediate node will be discarded and alarm message is broadcasted and isolate the detected node from network. This method has an increased end to end delay and routing overhead. This method is inefficient, if the black hole nodes work as a group in an attempt to drop packets.

Mohammad Al-Shurman[3] proposed the two methods to avoid the black hole attacks. According to the first solution, the source node verifies the validity of the route by finding more than one route to the destination. It waits for RREP packets to arrive from more than two nodes. The source node can recognize the safe route, when the source node receives RREP packets and the routes to destination have shared hops. This method causes routing delay. The second solution is to store the last packet sent sequence number and the last packet received sequence number in a table. When node receives reply message from another node it checks the last sent and received sequence number. If there is any mismatch, then the ALARM packet is broadcasted which indicates the existence black hole node. This mechanism is reliable and faster having no overhead.

LathaTamilselvan[8] proposed a solution in which the source node waits for the response including the next hop details from other neighboring nodes for a pre-defined time period. After time-out, it first checks in the CRRT (Collect Route Reply Table) table for any repeated next-hop-node. In the reply paths, if any repeated next-hop node is present, it assumes the chance of malicious paths is limited or the paths are correct. The solution adds a delay and the process of finding repeated next hop is an additional overhead.

MahaAbdelhaq, Sami Serhan, RaedAlsaqour and Rosilah Hassan[9] provide an improvement over the solution given in the paper[13] in which Source Intrusion Detection (SID) method is used. The SID mechanism proves to be viable solution for small scale MANET but when this mechanism is applied in a large scale MANET and the distance between the source node and the intermediate node is long, then the above solution is not sufficient. Furthermore, if the distance

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 6, June 2014

between the source node and the intermediate node is long, it will cause a prolonged delay in the discovery period of the route, which causes an overall network performance degradation. In order to mitigate the drawbacks in SID security routing mechanism, a new mechanism called Local Intrusion Detection (LID) security routing mechanism is proposed to allow the detection of the attacker to be locally; which means that when the suspected intermediate node unicast the RREP towards the source node, the previous node to the intermediate node performs the process of detection and not the source node.

YiebeltalFantahunAlem, Zhao ChenhXuan[5] proposed an Intrusion Detection using Anomaly Detection (IDAD) technique to prevent the black hole attack. IDAD assumes every activities of a user or a system can be monitored and anomaly activities of an intruder can be identified from normal activities. Hence, by identifying abnormal activities, it is possible to detect a possible intrusion and isolate the conflict. To do so an IDAD needs to be provided with a pre-collected set of unexpected activities, called audit data. Once audit data is collected and is given to the IDAD system, the IDAD system can compare the every activity of a host with the audit data on a fly. The IDAD system isolates the particular node by forbidding further interaction, if any activity of a host (node) resembles the activities listed in the audit data. It minimizes the extra routing packets which in turn minimizes the network overhead and facilitates faster communication.

S.Marti, T.J.Giuli, K.lai and M.bakery[11] proposed the Watchdog/Pathrater as a solution to the problem of selfish (or "misbehaving") nodes in MANET using DSR protocol. The Watchdog method is used to detect misbehaving nodes to respond the intrusion by isolating the selfish node from the network operation. Watchdog runs on each node. When a node forwards a packet, the nodes watchdog module verifies that the next node in the path also does so. The Watchdog achieves this by listening in promiscuous mode to the next nodes transmissions. If the packet is not forwarded by the next node, then it is considered as a misbehaving node and is reported. The Path rater module uses the information generated by Watchdog to select a better route to deliver the packets, avoiding the selfish nodes. K. Lakshmi enhances the AODV protocol. In AODV protocol, the destination sequence number is 32-bit integer associated with every route and is used to decide the freshness of a particular route. If the sequence number is largest, the route will be fresh enough. In this method, all the sequence numbers mentioned in RREP packet is stored along with the corresponding node ID in a RR-table (Route Request). Then, if the first destination sequence number in table is much greater than the sequence number of source node. That node will be identified as malicious node and the entry will be immediately removed from the table. The proposed solution also maintains the identity of the malicious node as MN-Id, hence enabling to discard the control messages from that node. Additionally, there is no need to forward the control messages from that malicious node. Moreover, in order to maintain freshness, the RR-Table is flushed once a route request is chosen from it.

III. ATTACKS IN MANET

A. *Black hole Attack:*

In this attack [9], an attacker advertises a zero metric for all destinations causing all nodes around it to route packets towards it. Fake routing information is sent by a malicious node, claiming that it has an optimum route which causes other good nodes to route data packets through the malicious one. All the packets received by the destructive node are dropped, instead of normally forwarding those packets.

In Black hole attack a malicious node may advertise a fresh path to a destination during routing process. The intention of the node may be to disturb the path finding process or interpret the packet being sent to destination. For example, in AODV, the attacker can send a fake RREP (including a fake destination sequence number that is fabricated to be equal or higher than the one contained in the RREQ) to the originating node, claiming that it has a sufficiently fresh route to the destination node, hence causing the originating node to select the route that passes through the destructive node resulting in all traffic being routed through the attacker. Therefore, the attacker can misuse or discard the traffic. The method how malicious node fits in the data routes varies. Figure below shows how black hole problem arises, here node "A" want to send data packets to node "D" and initiate the route discovery process. So if node "C" is a malicious node then it will claim that it has active route to the specified destination as soon as it receives RREQ packets. It will then send the response to node "A" before any other node. In this way node "A" will think that this is the active route

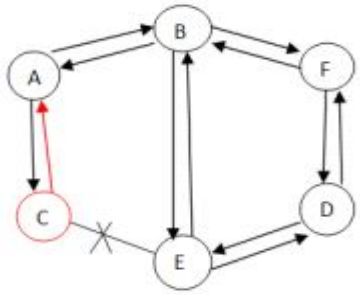
ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 6, June 2014

and thus active route discovery is complete. Node "A" will ignore all other replies and will start seeding data packets to node "C". In this way all the data packet will be lost consumed or lost [13].



Black Hole Attack

B. ***Gray-hole attack:***

This attack is also known as routing misbehaviour attack which leads to packet drops. It is a two-stage stage. The node advertise itself as having a valid route to destination during the first stage, while in second stage, nodes drop intercepted packets with a certain probability. The Grayhole attack has two phases:

Phase 1:

A malicious node exploits the AODV protocol to advertise itself as having a valid route to destination node, with the intention of interrupting packets of spurious route.

Phase 2:

In this phase, the nodes has been dropped the interrupted packets with a certain probability and the detection of Grayhole attack is a difficult process. Normally in the Grayhole attacks the attacker behaves maliciously for the time until the packets are dropped and then switch to their normal behaviour. Both normal node and attacker are same. Due to this behaviour it is very hard to find out in the network to figure out such kind of attack. The other name for Grayhole attack is node misbehaving attack [12].

C. ***Flooding attack:***

In flooding attack [9], attacker exhausts the network resources, such as bandwidth and to consume a node's resources, such as computational and battery power or to disrupt the routing operation to cause severe degradation in network performance. For example, in AODV protocol, a malicious node can send a large number of RREQs in a short period to a destination node that does not exist in the network. Because no one will reply to the RREQs, these will flood the whole network. As a result, all of the node battery power, as well as network bandwidth will be consumed and could lead to denial-of-service.

D. ***Wormhole Attack:***

In wormhole attack [14], a malicious node receives packets at one location in the network and tunnels them to another location in the network, where these packets are resent into the network. This tunnel between two colluding attackers is referred to as a wormhole. It could be established through wired link between two colluding attackers or through a single long-range wireless link. In this form of attack the attacker may create a wormhole even for packets not addressed to itself because of broadcast nature of the radio channel.

E. ***Blackmail:***

The blackmail attack [9] incurs due to lack of authenticity and it grants provision for any node to corrupt other node's legitimate information. Nodes usually keep information of perceived malicious nodes in a blacklist. This attack is relevant against routing protocols that use mechanisms for the identification of malicious nodes and propagate

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 6, June 2014

messages that try to blacklist the offender. An attacker may fabricate such reporting messages and tell other nodes in the network to add that node to their blacklists and isolate legitimate nodes from the network.

IV. CONCLUSION AND FUTURE WORK

As the use of mobile ad hoc networks (MANETs) has increased, the security in MANETs has also become more important accordingly. Due to the dynamic topology of MANETs, routing protocols are prone to various DoS attacks. In this paper, one can see the various types of attacks on mobile ad-hoc networks. This paper outlines characteristics of various attacks that can be considered while designing the security measures for ad hoc networks .By investigating these attacks and their characteristics one can design new security measures or protocols to protect MANETs.

REFERENCES.

1. C. E. Perkins and P. Bhagwat., "Highly Dynamic Destination-Sequenced Distance Vector Routing (DSDV) for Mobile Computers".
2. C. E. Perkins and E. M. Royer, "Ad-hoc On-Demand Distance Vector Routing".
3. DanaiChasaki and Tilman Wolf, "Evaluation of Path Recording Techniques in Secure MANET"s.
4. H. Tian and H. Shen, "Multicast-based Inference of Network-Internal Loss Performance," In Proc. of 7th International Symposium on Parallel Architectures, Algorithms and Networks (ISPAN 2004), Hong Kong, China, Vol.6 pp. 288–293, May 2004.
5. Dr.S.S.Tyagi and Aarti,"Study of MANET: Characteristics, Challenges, Application and Security Attacks",International Journal of Advanced Research in Computer Science and Software Engineering, Vol.3,Issue 5, May 2013.
6. IRACST – International Journal of Computer Networks and Wireless Communications (IJCNWC), ISSN: 2250-3501 Vol.2, No6, December 2012
7. J. Liebeherr, J. Wang, and G. Zhang. Programming overlay networks with overlay sockets. In Proc. 5th COST 264 Workshop on Networked Group Communications (NGC 2003), LNCS 2816, Vol.7,Issue 4, pp. 242–253, Sep. 2003.
8. LathaTamilselvan and V Sankarnarayana, "Prevention of Black Hole Attack in MANET", Journal of Networks, Volume 3, Number 5, 2008, pp 13-20.
9. Manjit Singh and GaganpreetKaur, "A Surveys of Attacks in MANET" International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 6, June 2013.
10. N. G. Duffield and F. Lo Presti, "Network tomography from measured end-to-end delay covariance", IEEE/ACM Transactions on Networking, Vol.12, Issue 6, pp. 978–992, Dec. 2004.
11. S.Marti, T.J.Giuli, K.lai and M.bakery "Mitigating routing misbehaviour in mobile ad hoc networks", 6thMobiCom, August 2000.
12. VineethaS. H. and ShebinKurian, "Performance Analysis of Cluster Based Secure Multicast Key Management in MANET", International Journal of Computer Science and Telecommunications, Vol.4, Issue 4, pp.1-14, April 2013.
13. Sheenu Sharma and Dr. Roopam Gupta, "Simulation Study Of Blackhole Attack in the Mobile Ad hoc Networks"
14. Abhay Kumar Rai, Rajiv RanjanTewari&Saurabh Kant Upadhyay, "Different Types of Attacks on Integrated MANET-Internet Communication"
15. V. SHANMUGANATHAN and Mr.T.ANAND M.E.,"A Survey on Gray Hole Attack in MANET" IRACST- International Journal of Computer Networks and Wireless Communications (IJCNWC), Vol.2, No6, December 2012 ISSN: 2250-3501.